**Check Pointin haittaohjelmakatsaus 8/2018**

**Reitittimien haavoittuvuudet houkuttelevat nyt kyberrikollisia**

*Tietoturvayhtiö Check Pointin keräämien tietojen mukaan verkkolaitteiden haavoittuvuuksia hyödyntävien haittaohjelmien esiintyvyys on yli kaksinkertaistunut toukokuun jälkeen.*

**ESPOO — 16. elokuuta 2018.** Check Pointin heinäkuun haittaohjelmatilasto näyttää nousua eritysesti verkkolaitteiden haavoittuvuuksien hyödyntämisessä.

Käytetyimpien haavoittuvuuksien globaalille Top 10 -listalle nousivat *MVPower DVR router Remote Code Execution* sijalle 5, *D\_Link DSL-2750B router Remote Command Execution* sijalle 7 ja *Dasan GPON router Authentication Bypass* sijalle 10. Näitä haavoittuvuuksia hyödyntäviä hyökkäyksiä koettiin heinäkuussa 45 prosentissa organisaatioista. Kesäkuussa vastaava luku oli 35 prosenttia ja toukokuussa 21 prosenttia.

Haavoittuvuuksien kautta hyökkääjä voi ujuttaa laitteelle haittaohjelman, jonka avulla laitteen voi ottaa hallintaan. Tyypillisiä modeemin tai reitittimen kautta verkossa oleviin laitteisiin eteneviä haittaohjelmia ovat Mirai, IoTroop/Reaper ja VPN Filter.

”Haavoittuvuudet takaavat kyberrikollisille helpon ja suhteellisen kitkattoman pääsyn yritysverkkoihin, mikä puolestaan mahdollistaa monenlaista pahantahtoista toimintaa. IoT-laitteiden kautta on usein yksinkertaista tunkeutua muihin verkkoon liitettyihin laitteisiin. Siksi on tärkeää, että laitteiden ohjelmistot päivitetään heti, kun ilmi tulleeseen haavoittuvuuteen on tarjolla paikkaava päivitys”, tietoturvatutkijoiden ryhmää Check Pointilla vetävä Threat Intelligence Group Manager **Maya Horowitz** kommentoi.

”Yritysverkko on mahdollista ja suositeltavaa suojata sekä tunnetuilta että tuntemattomilta haavoittuvuuksilta monikerroksisen verkkotietoturvastrategian avulla”, Horowitz lisäsi.

Coinhive oli heinäkuussa edelleen maailman yleisin haittaohjelma. Se vaikutti 19 prosenttiin organisaatiosta. Cryptoloot ja Dorkbot sijoittuivat toiseksi ja kolmanneksi, ja kummankin globaali vaikutus oli 7 prosenttia.

**Suomen yleisimmät haittaohjelmat heinäkuussa Top 5:**

1. **Coinhive** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.
2. **Roughted** – Laajan skaalan haittamainosohjelma, voi tarjota reitin myös kiristysohjelmille.
3. **Cryptoloot** – Kryptovaluuttalouhija, Coinhiven kilpailija**.**
4. **Dorkbot** – Pankkitroijalainen, joka urkkii uhrin tietoja ja jota käytetään usein myös palvelunestohyökkäysten toteuttamiseen.
5. **Jsecoin** – Kryptolouhija, jota käytetään yleensä verkkosivustolle istutettuna. Sallimalla louhinnan voi ostaa esimerkiksi mainoksetonta aikaa tai pelivaluuttaa.

**Maailman yleisimmät haittaohjelmat heinäkuussa Top 3:**

*\*Nuoli osoittaa muutoksen listasijoituksessa edelliseen kuukauteen verrattuna*

1. **↔ Coinhive** – Kryptolouhija, joka on suunniteltu louhimaan Moneroa käyttäjän tietämättä, kun tämä vierailee verkkosivulla.
2. **↔ Cryptoloot** – Kryptolouhija, joka käyttää uhrin prosessoritehoa kryptovaluutan louhimiseen.
3. **↔** **Dorkbot** – Pankkitroijalainen, joka urkkii uhrin tietoja ja jota käytetään usein myös palvelunestohyökkäysten toteuttamiseen.

**Maailman yleisimmät mobiililaitteiden haittaohjelmat heinäkuussa Top 3:**

1. **Lokibot** - Android-laitteiden pankkitroijalainen, joka voi myös muuntua kiristysohjelmaksi lukiten puhelimen.
2. **Triada** - Android-laitteiden takaovi, joka myöntää superkäyttäjäoikeudet haittaohjelmien lataamiseen.
3. **Guerilla** - Tuo mainoksia puhelimelle ja klikkailee niitä ilman käyttäjän suostumusta.

**Maailman hyödynnetyimmät haavoittuvuudet heinäkuussa Top 3:**

1. **↔ Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow (CVE-2017-7269**
2. **↑ Apache Struts2 Content-Type Remote Code Execution (CVE-2017-5638**)
3. **↑ OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160; CVE-2014-0346)**

Kuukausittain laadittava haittaohjelmatilasto perustuu Check Pointin ThreatCloudinTM tietoihin. Se on maailman laajin verkosto, joka kerää tietoja kyberhyökkäyksistä ja näyttää ne reaaliaikaisesti kartalla. Verkosto tunnistaa päivittäin miljoonia haittaohjelmatyyppejä analysoidessaan yli 250 miljoonasta verkko-osoitteesta saamiaan tietoja.

Täydellinen Top 10 -haittaohjelmalista löytyy Check Pointin blogista osoitteesta

<http://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/>

Check Pointin uhkientorjuntaresurssit ovat saatavilla osoitteesta <http://www.checkpoint.com/threat-prevention-resources/index.html>

**Lisätiedot ja haastattelupyynnöt:**

Maajohtaja Robert Lindqvist, Check Point Software Technologies, [robertl@checkpoint.com](mailto:robertl@checkpoint.com), p. 050 368 4912

OSG Viestintä, Maija Rauha, [maija.rauha@osg.fi](mailto:maija.rauha@osg.fi), p. 0400 630 065

**Seuraa Check Pointia:**

Twitter: <http://www.twitter.com/checkpointsw>

Facebook: <https://www.facebook.com/checkpointsoftware>

Blog: <http://blog.checkpoint.com>

YouTube: <http://www.youtube.com/user/CPGlobal>

LinkedIn: <https://www.linkedin.com/company/check-point-software-technologies>

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on maailman suurin tietoverkkojen kyberturvallisuuteen keskittynyt yhtiö. Se tarjoaa alan johtavia ratkaisuja ja suojelee asiakkaitaan kyberhyökkäyksiltä vertaansa vaille olevalla haittaohjelmien, kiristysohjelmien ja muiden tietoturvan uhkien kiinnijäämisprosentilla. Check Pointin kattava tietoturva-arkkitehtuuri suojaa niin yrityksen verkot, pilvipalvelut kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava ja intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta.